

UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with all Google accounts, fully  
described in Attachment A.

Case No. 19-M-059

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Information associated with all Google accounts, fully described in Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

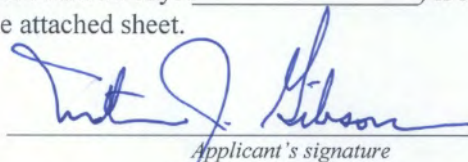
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 2113(a) (Bank Robbery) and 18 U.S.C. § 924(c) (Brandishing a Firearm During a Crime of Violence)

The application is based on these facts: See attached affidavit.

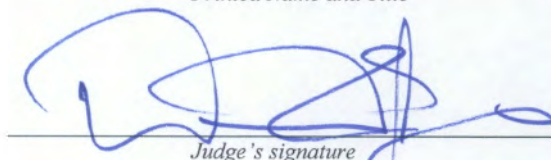
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Matthew Gibson, FBI Task Force Officer  
Printed Name and Title

Sworn to before me and signed in my presence:

Date: April 15, 2019

  
Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Matthew Gibson, being first duly sworn on oath, on information and belief state:

**I. INTRODUCTION, BACKGROUND, TRAINING, AND EXPERIENCE:**

1. I make this affidavit in support of an application for a search warrant for information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Attachment B.

2. I have over 27 years of experience as a law enforcement officer and am currently assigned to the Milwaukee FBI Violent Crime Task Force as a Deputized Federal Task Force Officer. I was a Special Agent with the Federal Bureau of Investigation for over 23 years and have been an Investigator with the Milwaukee County District Attorney's Office since 2015. I have participated in numerous complex narcotics, money laundering, violent crime, armed bank robbery, and armed commercial robbery investigations in violation of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, and Title 18, United States Code, Sections 924(c), 1951, 1956, 1957, 2113, and other related offenses. I have employed a wide variety of investigative techniques in these and other investigations, including but not limited to, the use of informants, wiretaps, cooperating defendants, recorded communications, search warrants, surveillance, interrogations, public records, DNA collection, and traffic stops. I have also received formal training regarding the same. As a Federal Task Force Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. Based on the facts set forth in this affidavit, there is probable cause to search the information described in Attachment A for evidence of a violation of in violation of 18 U.S.C. § 2113(a) (Bank Robbery) and 18 U.S.C. § 924(c) (Brandishing a Firearm During a Crime of Violence).

4. This affidavit is based upon my training and experience, my personal knowledge and information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon police reports, surveillance videos, and witness statements, that I consider to be reliable as set forth herein.

5. Because this affidavit is submitted for the limited purpose of a obtaining a search warrant, I have not included each and every fact known to me concerning this investigation.

## **II. JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense investigated.” 18 U.S.C. § 2711(3)(A)(i).

## **III. BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY**

7. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called “cells,” enabling communication with other cellular telephones or traditional “landline” telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

8. Google is an Internet company which, among other things, provides electronic communication services to subscribers. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretreived email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including



whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. Further, information maintained by the email provider can show how, where, and when the account was accessed or used. Based on my training and experience, I have learned that Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user's Internet browser.

12. Google has developed an operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account and users are prompted to add a Google account when they first turn on a new Android device.

13. Over the past 15 years the majority of subjects I have arrested and investigated have had cellular telephones and utilized them in some capacity in furtherance of their criminal activity, such as but not limited to; arranging meetings with co-conspirators; taking photographs of bank proceeds, firearms, and vehicles used in robberies; using Instant Messaging and Facebook posts to sell pills stolen from pharmacies; purchasing firearms which were used in robberies; using web searches to find pharmacies and cellular phone stores they later robbed; and sending text messages concerning robberies. Additionally, in numerous police reports I have reviewed as part of these criminal investigations the subjects almost always have a cellular telephone mentioned in the report or seized as evidence.

14. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. The company uses this information for location-based advertising and location-based search results. This information is derived from GPS data, cell site/cell tower information, and Wi-Fi access points.

15. Location data can assist investigators in understanding the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

#### **IV. PROBABLE CAUSE**

16. On March 22, 2018, two unidentified masked male subjects (Subject #1 and Subject #2) committed the armed robbery of the TCF Bank, located at 1815 63<sup>rd</sup> Street, Kenosha,

Wisconsin. Both Subjects were brandishing firearms as they entered the bank at approximately 9:20 a.m. Both Subjects were yelling for everyone to get on the ground. Both Subjects jumped over the teller counter and demanded money from different employees. Subject #1 demanded money be placed into a bag. Each Subject specified that they did not want any bank security devices. After obtaining the money the Subjects demanded the employees get on the floor and count to ten. The Subjects both fled the bank. Surveillance video captured them running between two residences and out of sight.

17. Witness statements and surveillance video indicated Subject #1 was a black male, approximately 5'9" tall, in his 20s, wearing a maroon hooded sweatshirt, gloves, yellow bandana over his face and a baseball hat. Subject #1 was armed with a handgun. Subject #2 was described as a black male, approximately 5'9" tall, in his 20s, wearing all dark clothing which included a hooded sweatshirt with white paint splashes and an American flag on the left shoulder, gloves, a dark colored bandana covering his face, a black stocking cap with a thin light colored stripe. Subject #2 was armed with a black and silver handgun. The Subjects walked between the houses located at 1818 and 1820 63<sup>rd</sup> Street, Kenosha, Wisconsin on their way to rob the bank.

18. On January 23, 2019, at approximately 11:22 a.m., officers responded to the armed robbery at the TCF Bank, 1815 63<sup>rd</sup> Street, Kenosha, Wisconsin. Witness statements and surveillance video indicated that two masked unknown subjects entered that bank. The first subject who entered the bank (Subject #1) displayed a silver semi-automatic handgun and confronted the security guard sitting near the bank entrance. At gunpoint, Subject #1 forced the security guard to move closer to the teller counter and demanded he get on the floor. Subject #1 placed the firearm to the back of the guard's head and began counting down from 15. When Subject #1 got to 10 he

yelled, "Hurry up or I'm going to blow his head off." Subject #2 had already jumped over the teller counter and produced a small black plastic bag and repeatedly stated he did not want any dye packs. Money was placed into the black bag. After obtaining money, both subjects demanded the victims get on the floor. Witnesses again heard them counting down as they fled the bank. The subjects ran northwest from the bank and ran between two houses on the west side of the street, 1908 and 1910 63<sup>rd</sup> Street, Kenosha, Wisconsin.

19. Subject #1 was described as a black male, mid 20's, approximately 5'8" to 5'11" tall, thin build, light complexion, armed with a silver handgun. Wearing a blue and gray marbled hooded sweatshirt, a black mask, gloves, light colored jeans, light colored athletic shoes. Subject #2 was described as a black male, mid 20's, approximately 5'4" tall, thin build, wearing a black hooded sweatshirt with a blue hood over a white shirt, blue mask, gloves, blue sweatpants, and dark colored athletic shoes.

20. Investigators believe similarities between the two robberies described above indicate that the incidents may have been committed by the same subjects or group of subjects. Both robberies contain the following pieces of similar information: same bank in each incident; there were two Subjects for each incident; the Subjects were armed and displayed firearms; the Subjects demanded the victims get on the floor; the Subjects jumped over the teller counter; the Subjects used a bag; the Subjects counted down to gain compliance; the Subjects repeatedly referred to bank security devices; the Subjects wore hooded sweatshirts; the Subjects wore gloves; the Subjects wore masks; the Subjects demanded employees get on the floor prior to the subjects fleeing from the bank; and the Subjects came from and/or fled northward from the bank.

21. Google Maps identified the TCF Bank, 1815 63<sup>rd</sup> Street, Kenosha, Wisconsin, location using latitude/longitude data as 42.577401, -87.831823.



22. According to the Statcounter website, <http://gs.statcounter.com/os-market-share/mobile/united-states-of-america>, as of March 2019, the Apple operating system iOS and the Android Operating System account for 99% of the US market share of Mobile operating systems.

23. Based on my training and experience I know that robbery suspects often use utilize mobile cellular devices as tools in furtherance of their robbery conspiracies. For example, I know that robbery suspects often use accomplices as lookouts or getaway drivers and communicate with these accomplices through cell phones. Often times, suspects conduct pre-robbery surveillance to determine the number of people inside of the store or the presence of law enforcement.

## **V. CONCLUSION**

24. Based on the forgoing, it is probable that the unknown subjects of this investigation had cellular telephones which utilized either Google's Android or Apple OIS operating systems. I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable probable cause exists to permit the execution of the requested warrant at any time in the day or night.

## **VI. REQUEST FOR SEALING**

25. It is further requested that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

### BANK ROBBERY LOCATION

This warrant applies to information associated with all Google accounts that, during the **time period** described below, were accessed from a mobile device located in the **geographic region** described below.

- This warrant calls for information that is stored at premises controlled by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.



ATTACHMENT A2

BANK ROBBERY LOCATION

**BANK ROBBERY LOCATION**

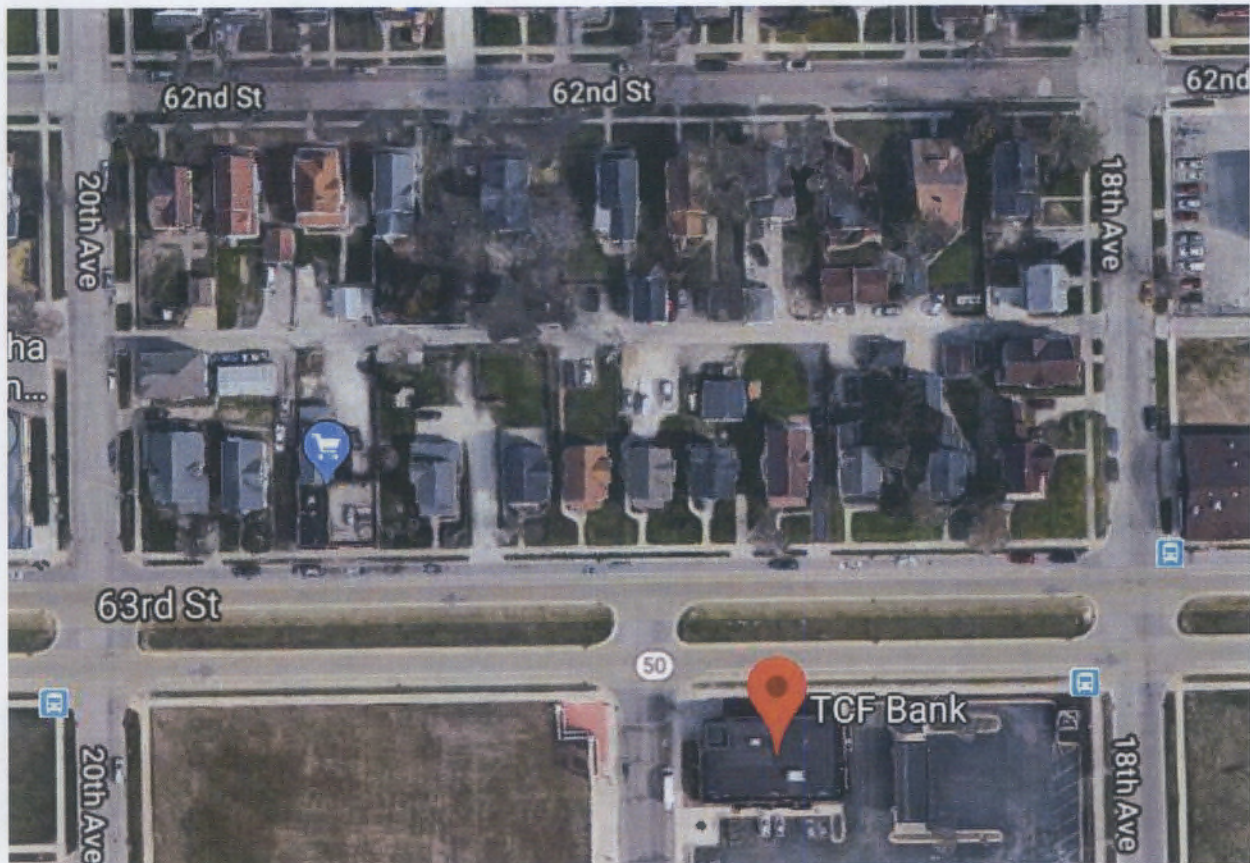
Latitude/Longitude: 42.577401, -87.831823

TCF Bank, 1815 63rd Street, Kenosha, WI

**Area Borders:**      42.577203, -87.833431 - Southwest Corner  
                             42,578546, -87.833431 – Northwest Corner  
                             42.578546, -87.830942 – Northeast Corner  
                             42.577203, -87.830942 – Southeast Corner

42,578546, -87.833431

42.578546, -87.830942



42.577203, -87.833431

42.577203, -87.830942

## **ATTACHMENT B**

### ***Particular Things to be Seized***

#### **I. Information to be disclosed by Google (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider shall provide responsive data (as described in Attachments A1 and A2) pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters (as described in Attachments A1 and A2).
2. For each location point recorded within the Initial Search Parameters, Google shall produce anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the “Anonymized List”).
3. Law enforcement shall review the Anonymized List to remove devices that are not relevant to the investigation, for example, devices that were not in the location for a sufficient period of time. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the Time Period that fall outside of the Target Location. These contextual location coordinates may assist law enforcement in identifying devices that were located outside the Target Location, were not within the Target Location for a long enough period of time, were moving through the Target Location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.
4. For those device IDs identified as relevant pursuant to the process described above, law enforcement may request that Google provide subscriber information for the Google account associated with each identified device ID.